

①⑨ BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

⑫ **Offenlegungsschrift**  
⑪ **DE 3041 109 A 1**

⑤① Int. Cl. 3:  
**G06K 19/06**  
G 07 C 9/00  
G 07 F 7/08

②① Aktenzeichen:  
②② Anmeldetag:  
④③ Offenlegungstag:

P 30 41 109.7  
31. 10. 80  
9. 6. 82

*Beihördeneigentum*

⑦① Anmelder:  
GAO Gesellschaft für Automation und Organisation mbH,  
8000 München, DE

⑦② Erfinder:  
Obrecht, Werner, 8121 Wielenbach, DE

⑤④ Identifikationselement

DE 3041 109 A 1

DE 3041 109 A 1

K 13099 / 41 143

GAO Gesellschaft für Automation  
und Organisation mbH  
Euckenstr. 12  
8000 München 70

---

Identifikationselement

---

P a t e n t a n s p r ü c h e

1. Identifikationselement, insbesondere für Ausweis-  
karten und ähnliche Datenträger, das neben allgemeinen  
Daten einen Identifikationscode enthält, der bei jeder  
Benutzung des betreffenden Datenträgers mit einem  
5 beispielsweise manuell eingegebenen Code zur Bildung  
einer Ja/Nein-Aussage verglichen wird, dadurch g e -  
k e n n z e i c h n e t, daß das Identifikationsele-  
ment mindestens ein aktivierbares Zeitglied (1,2) ent-  
hält, durch das im Anschluß an die Code-Eingabe die  
10 Kommunikation mit dem Element für einen vorgegebenen  
Zeitraum beeinflufßbar ist.

- 2 -

2. Identifikationselement nach Anspruch 1, dadurch  
g e k e n n z e i c h n e t, daß das aktivierbare  
Zeitglied ein Sperrglied (1) ist, das im Anschluß  
an eine falsche Code-Eingabe die Kommunikation mit  
5 dem Identifikationselement für einen vorgegebenen  
Zeitraum blockiert.

3. Identifikationselement nach Anspruch 1, dadurch  
g e k e n n z e i c h n e t, daß das aktivierbare  
10 Zeitglied ein Freigabeglied (2) ist, das im Anschluß  
an eine richtige Code-Eingabe die Kommunikation  
mit dem Identifikationselement für einen vorgege-  
benen Zeitraum ermöglicht.

4. Identifikationselement nach Anspruch 2 und 3, da-  
durch g e k e n n z e i c h n e t, daß das Iden-  
tifikationselement sowohl ein Sperrglied (1) als  
auch ein Freigabeglied (2) enthält, die komplementär  
betrieben werden.

20 5. Identifikationselement nach einem der Ansprüche  
1 bis 4, dadurch g e k e n n z e i c h n e t, daß  
das Zeitglied (1,2) aus einem Ladungselement (3)  
und einem Steuerelement (4) besteht.

25 6. Identifikationselement nach Anspruch 5, dadurch  
g e k e n n z e i c h n e t, daß das Ladungselement (3)  
ein in der Technologie des integrierten Schalt-  
kreises hergestellter Kondensator ist.

30 7. Identifikationselement nach Anspruch 5, dadurch  
g e k e n n z e i c h n e t, daß das Ladungselement (3)  
eine in der "Floating-Gate-Technik" hergestellte  
Speicherzelle ist.

ORIGINAL INSPECTED

8. Identifikationselement nach Anspruch 7, dadurch  
g e k e n n z e i c h n e t, daß das Ladungselement (3)  
mit einer UV-absorbierenden Schicht abgedeckt ist,  
die bei Entfernung zwangsläufig zu einer Zerstörung  
5 des Elements (3) führt.

9. Identifikationselement nach einem der Ansprüche 5  
bis 8, dadurch g e k e n n z e i c h n e t, daß das  
Steuerelement ein als Impedanzwandler geschalteter  
10 Operationsverstärker (9) ist, der abhängig von der  
Ladung des Ladungselements (7) ein Steuersignal abgibt.

10. Identifikationselement nach Anspruch 9, dadurch  
g e k e n n z e i c h n e t, daß im Ladestromkreis  
15 des Ladungselements (7) eine in Durchlaßrichtung ge-  
schaltete Diode (8) vorgesehen ist, die das Ladungs-  
element (7) im Ladezustand von der Ansteueranordnung  
(5,6) entkoppelt.

20 11. Identifikationselement nach Anspruch 9 oder 10,  
dadurch g e k e n n z e i c h n e t, daß in der  
Versorgungsleitung des Zeitgliedes (1,2) ein weiteres  
Ladungselement (12) vorgesehen ist, das den Anfangs-  
ladestrom des das Steuersignal beeinflussenden La-  
25 dungselementes (7) kompensiert.

12. Identifikationselement nach einem der Ansprüche  
9 bis 11, dadurch g e k e n n z e i c h n e t, daß  
in der Versorgungsleitung des Zeitgliedes (1,2) zu-  
30 sätzliche Dioden (13,14) vorgesehen sind, die den  
Einfluß einer Umpolung der Versorgungsspannung  
kompensieren.

13. Identifikationselement nach Anspruch 9 oder 10,  
dadurch g e k e n n z e i c h n e t, daß parallel  
zum das Steuersignal beeinflussenden Ladungselementes (7)  
ein weiteres Ladungselement (15) vorgesehen ist, das  
5 bei jeder Inbetriebnahme des Identifikationsele-  
mentes aufladbar ist und das über ein entsprechend  
angesteuertes Schaltelement (18) beim Auftreten eines  
Fehlersignals seine Ladung an das das Steuersignal  
beeinflussende Ladungselement (7) abgibt.
- 10 14. Identifikationselement nach einem der vorher-  
gehenden Ansprüche, dadurch g e k e n n z e i c h -  
n e t, daß zusätzlich ein rückstellbarer Zähler (20)  
vorgesehen ist, der erst nach mehrmaligem Auftreten  
15 eines Fehlersignals das Zeitglied (1,2) ansteuert.
15. Identifikationselement nach einem der vorhergehen-  
den Ansprüche, dadurch g e k e n n z e i c h n e t,  
daß es zusätzlich einen Schwellwertschalter (21)  
20 aufweist, der das Zeitglied (1,2) bei Unterschreitung  
der Versorgungsspannung unterhalb eines vorgegebenen  
Werts ansteuert.
- 25 16. Identifikationselement nach einer der vorhergehen-  
den Ansprüche, dadurch g e k e n n z e i c h n e t,  
daß die Code-Eingabe in das Identifikationselement  
mit Hilfe eines Taschenterminals durchführbar ist.
- 30 17. Identifikationselement nach Anspruch 16, dadurch  
g e k e n n z e i c h n e t, daß das Taschenterminal  
eine Anzeige aufweist, mit der die Betriebsbereit-  
schaft des Identifikationselements sichtbar gemacht  
werden kann.

Die Erfindung betrifft ein Identifikationselement, insbesondere für Ausweiskarten und ähnliche Datenträger, das neben allgemeinen Daten einen Identifikationscode enthält, der bei jeder Benutzung  
5 des betreffenden Datenträgers mit einem beispielsweise manuell eingegebenen Code zur Bildung einer Ja/Nein-Aussage verglichen wird.

Identifikationselemente der oben genannten Art werden  
10 in Form integrierter Schaltkreise in Ausweiskarten oder ähnliche Datenträger eingebaut, die in letzter Zeit zunehmend im automatischen Geld- und Dienstleistungsverkehr zum Einsatz kommen. Um nur dem Eigentümer der Ausweiskarte die Benutzung zu ermöglichen,  
15 enthält das Identifikationselement einen nur ihm bekannten vertraulichen Code, welcher beispielsweise die Form einer vierstelligen Ziffer aufweisen kann, die bei jeder Benutzung der Karte mit einer vom Benutzer über ein geeignetes Terminal eingegebenen  
20 Ziffer verglichen wird. Nur wenn die Zeichenfolgen der beiden Ziffern übereinstimmen, kann die Ausweiskarte tatsächlich genutzt werden, um beispielsweise von einem Konto Geld abzuheben.

25 Falls eine mit einem derartigen Identifikationselement versehene Karte gestohlen wird oder verlorengeht, bietet sich grundsätzlich einem mit der Materie vertrauten Betrüger die Möglichkeit, den vertraulichen Code dadurch in Erfahrung zu bringen, daß er mit  
30 Hilfe eines geeigneten Programms und entsprechend

hoher Zyklusfrequenzen alle Code-Möglichkeiten innerhalb kurzer Zeit durchspielt und die Reaktion des Identifikationselements auf den richtigen Code auswertet. Dabei kommt dem Betrüger die Tatsache  
5 zugute, daß der Code, der für den Benutzer leicht merkbar sein soll, in den meisten Fällen aus nur wenigen Zeichen besteht.

Aus diesem Grunde ist bereits vorgeschlagen worden,  
10 die oben genannte Betrugsmöglichkeit durch einen sogenannten Fehlerzähler auszuschließen (siehe dazu US-PS 3 906 460 und DE-OS 26 21 271). Der Fehlerzähler registriert dabei jeden falsch eingegebenen Code und verhindert die Kommunikation bzw. zerstört  
15 die Anordnung, sobald eine vorgesehene Fehlerzahl erreicht ist. Gemessen an der Zahl der Code-Möglichkeiten wird in diesem Zusammenhang die Zahl der zulässigen Fehler so niedrig gewählt, daß der Betrüger praktisch keine Chance hat, den richtigen Code zu  
20 finden, während andererseits dem rechtmäßigen Benutzer über die gesamte Laufzeit der Karte hinweg einige versehentlich-begangene Fehler zugestanden werden.  
Die Fehler müssen dabei so gespeichert werden, daß der jeweilige Wert auch bei stromloser Anordnung erhalten bleibt und nicht manipulierbar ist. Entsprechend  
25 der DE-OS 26 21 271 werden deshalb als Fehlerzähler sogenannten nichtflüchtige Speicher vorgeschlagen, wobei als sicherste Form der irreversiblen Speicherung die Speicherung mit Hilfe sogenannter PROM's möglich ist,  
30 bei denen während der Programmierung entsprechende

Leiterbahnen durchgebrannt werden.

Die bisher bekannten, nichtflüchtigen Festkörperspeicher haben jedoch die Eigenschaft, daß während  
5 des Einspeichervorgangs, welcher, wie erwähnt, beispielsweise aufgrund des Durchbrennens von Leiterbahnen zustandekommt, zwangsläufig eine erhöhte Leistungsaufnahme über einen Zeitraum von einigen Millisekunden zustandekommt, woraus sich wieder Möglichkeiten ergeben, derartige Identifikationselemente zu manipulieren. Durch  
10 Überwachung der Stromaufnahme des Identifikationselements könnte nämlich ein Betrüger bei Registrierung eines erhöhten Wertes den Speichervorgang verhindern, indem er die Versorgungsspannung abschaltet. Im Rahmen der  
15 DE-OS 26 21 271 ist somit bereits vorgeschlagen worden, eine Simulationsschaltung vorzusehen, die bei jeder Code-Überprüfung eine erhöhte Leistungsaufnahme simuliert. Wird ein falscher Code ermittelt, schaltet eine geeignete Logik die Simulationsschaltung aus und  
20 leitet bei nahezu gleichbleibender Leistungsaufnahme den Speichervorgang ein.

Bei der Realisierung derartiger Schutzvorrichtungen zeigt sich jedoch, daß Fehlerzähler und alle zwangsläufig damit verbundenen Zusatzeinrichtungen einen  
25 erheblichen Schaltungsaufwand erfordern, der vor allem auch dem Bestreben widerstrebt, die Anordnung bzw. das Halbleiterplättchen für die o. g. Anwendung möglichst klein zu halten. Außerdem schränkt der Fehlerzähler die vorgesehene Gültigkeitsdauer der Aus-  
30



weiskarte unter Umständen stark ein, weil auch bei einer legitimen Benutzung Fehleingaben unvermeidbar sind. Dies gilt umsomehr, wenn der Benutzer einen stark frequentierten Geldausgabeautomaten aufsucht und die Bedienung unter Zeitdruck und gegebenenfalls von anderen Personen beobachtet vornehmen muß.

Die Aufgabe der vorliegenden Erfindung besteht somit darin, ein Identifikationselement der genannten Art zu schaffen, welches mit erheblich vermindertem Schaltungsaufwand die erwähnten Betrugsmöglichkeiten verhindert und welches eine für den Besitzer des Identifikationselements angenehme Benutzung zuläßt.

Die Aufgabe wird erfindungsgemäß dadurch gelöst, daß das Identifikationselement mindestens ein aktivierbares Zeitglied enthält, durch das im Anschluß an eine Code-Eingabe die Kommunikation mit dem Element für einen vorgegebenen Zeitraum beeinflussbar ist.

Der Grundgedanke der Erfindung besteht darin, daß ein zeitabhängiges und von der übrigen Schaltung des Identifikationselements entkoppeltes Element (Zeitglied) vorzusehen ist, mit welchem das Identifikationselement nach einer Fehleingabe für einen bestimmten Zeitraum funktionslos gemacht wird, indem beispielsweise die Dateneingangsleitung gesperrt wird. Es ist jedoch ebenso möglich, daß zusätzlich oder auch unabhängig von der erstgenannten Funktion ein Zeit-

glied verwendet wird, das die Benutzung des Identifikationselements nach einmaliger Code-Eingabe für einen bestimmten Zeitraum ohne weitere Code-Eingabe ermöglicht.

5

Bei der Nutzung des Zeitgliedes als Sperrelement ist es für dessen Funktion unerheblich, ob das Identifikationselement nach Erkennung einer Fehleingabe von der Versorgungsquelle abgetrennt wird oder nicht.

10 Das Zeitglied ist jedoch in jedem Fall innerhalb des Identifikationselements derart ausgebildet und elektronisch entkoppelt, daß die Sperrfunktion durch externe Mittel weder aufgehoben noch verändert werden kann. Erst wenn die Dateneingangsleitungen  
15 nach Ablauf der Sperrzeit wieder freigegeben werden, ist eine erneute Code-Eingabe und damit die weitere Kommunikation möglich.

In Abhängigkeit von den möglichen Code-Permutationen  
20 des gewählten Codes ist die Sperrzeit so bemessen, daß es für einen Betrüger praktisch unmöglich ist, während der vorgegebenen Gültigkeitsdauer der Karte den richtigen Code zu finden, womit durch eine einfache schaltungstechnische Maßnahme die oben  
25 genannten Betrugsmöglichkeiten beseitigt werden, während andererseits die vorgesehene Gültigkeitsdauer der Karte in vollem Umfang genutzt werden kann.

In vorteilhafter Weise kann das erfindungsgemäße  
30 Zeitglied auch in der Form eingesetzt werden, daß

ein richtig eingegebener Code den Betrieb des Identifikationselements für einen vorbestimmten Zeitraum ermöglicht. Damit wird der Benutzer in die Lage versetzt, schon vor der eigentlichen Transaktion, 5 unbehelligt und ungestört durch andere Personen, beispielsweise mit Hilfe eines Taschenterminals eine Code-Eingabe vorzunehmen. Bei der beispielsweise an einem Geldausgabeautomat vorgenommenen Transaktion selbst, entfällt dann die Code-Eingabe, so daß 10 innerhalb des vorbestimmten Zeitraums allein durch Eingabe des Identifikationselements in den entsprechenden Automaten die betreffende Transaktion ausgelöst wird. Ein Ausspähen des Codes durch fremde Personen wird damit unmöglich gemacht.

15 Die oben genannten Funktionen können alternativ aber auch, wenn im Identifikationselement zwei Zeitglieder vorgesehen sind, gemeinsam genutzt werden.

20 Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand der beigefügten Zeichnungen näher beschrieben.

25

Darin zeigen:

Fig. 1 ein Blockschaltbild mit dem gemäß der Erfindung vorgesehenen Zeitglied,

Fig. 2, 3, 4      detaillierte Ausführungsformen des  
Zeitgliedes von Fig. 1

5      Fig. 5      ein Blockschaltbild einer Anordnung  
mit zwei in komplementärer Betriebs-  
weise betriebenen Zeitgliedern und

Fig. 6      eine modifizierte Ausführungsform der  
Erfindung.

10

Fig. 1 zeigt beispielhaft in einem schematisierten  
Blockschaltbild den Aufbau des erfindungsgemäßen Zeit-  
gliedes, wie es in der integrierten Schaltung eines  
Identifikationselements enthalten sein kann. Das  
15      gezeigte Zeitglied 1 besteht aus einem Ladungselement  
3 in Form eines Ladungsspeichers und einem Steuer-  
element 4. Das Ladungselement 3 ist in einfachstem  
Fall ein Kondensator, der immer dann geladen wird,  
wenn von einem Komparator 5 her ein Signal zugeleitet  
20      wird. Der Komparator 5 vergleicht beispielsweise den  
über eine Tastatur eingegebenen Ist-Identifikations-  
Code mit dem im Identifikationselement gespeicherten  
Soll-Identifikations-Code und erzeugt ein Fehlersignal,  
wenn die Zeichenfolgen nicht übereinstimmen. Das mit  
25      dem Ladungselement 3 verbundene Steuerelement 4 er-  
zeugt bei geladenem Kondensator ein Ausgangssignal,  
mit dem die Kommunikation mit dem Identifikationsele-  
ment für einen vorbestimmten Zeitraum beeinflussbar  
ist. Diese Beeinflussung kann beispielsweise derart  
30      erfolgen, daß mit Hilfe des Ausgangssignals die

Dateneingangsleitung des Identifikationselements gesperrt wird, so daß es für den vorbestimmten Zeitraum funktionslos ist.

- 5 Das aus den Elementen 3 und 4 bestehende Zeitglied 1 kann in der Technik integrierter Schaltkreise, beispielsweise der MOS-Technik hergestellt sein. Jedoch kann auch die sogenannte "Floating-Gate-Technik" Verwendung finden, welche bei der Herstellung nicht-  
10 flüchtiger Speicher genutzt wird, die mit UV-Licht oder auch elektrisch löscher sind. Das Ladungselement 3 besteht in diesem Fall aus einer FET-Transistorzelle, in deren Steuereingang eine isolierte Ladungsinsel (Floating Gate) integriert ist, wobei  
15 je nach Ladungszustand der "Insel" die Schaltwelle des Transistors verändert wird. Dabei kann erreicht werden, daß ein einmal geladenes, programmiertes Ladungselement (Speicherzelle) die Ladung und damit den logischen Zustand über mehrere Jahre beibehält. Da  
20 die Entladezeit im wesentlichen durch die Art und Dicke der die Insel umgebenden Isolierschicht bedingt ist, kann durch Änderung der Parameter die Entladezeit so variiert werden, daß diese den der Erfindung zugrundeliegenden Erfordernissen angepaßt ist. Um  
25 ein unbefugtes Löschen eines derartigen Ladungselementes zu verhindern, müssen ferner entsprechende Maßnahmen vorgenommen werden. So kann beispielsweise eine durch UV-Strahlung löschbare Speicherzelle mit einem Material abgedeckt werden, das UV-Licht absorbiert. Das die Speicherzelle abdeckende Material  
30 wird dabei so angeordnet, daß eine Ent-

fernung zwangsläufig mit der Zerstörung der Zelle verbunden ist.

Die Fig. 2 zeigt eine detailliertere Ausführungsform  
5 der Erfindung. Mit dem Fehlerimpuls des Komparators  
5 wird in diesem Fall ein Gatter 6 angesteuert,  
dessen Ausgang nahezu auf Versorgungsspannung ansteigt  
und dabei einen Kondensator 7 über eine Diode 8 auflädt.  
Dieser Kondensator 7 ist mit einem als Impedanzwand-  
10 ler wirkenden Operationsverstärker 9 verbunden, der  
einen sehr hohen Eingangswiderstand aufweist. Das Aus-  
gangssignal des Operationsverstärkers 9 wird nach  
Invertierung genutzt, um ein Daten-Eingangsgatter  
10 zu sperren.

15 Damit ein Betrüger den richtigen Code finden kann,  
muß derselbe die Sperrzeit abwarten, bis das Identi-  
fikationselement für einen weiteren Codevergleich  
neue Daten aufnehmen kann. Abhängig von den möglichen  
20 Code-Permutationen wird die Sperrzeit so gewählt,  
daß ein Betrüger innerhalb der Gültigkeitsdauer  
des Identifikationselements praktisch keine Chance  
hat, den richtigen Code zu finden. In diesem Zusammen-  
hang kann folgende Gleichung aufgestellt werden:

25

$$T_e = \frac{N \cdot T_s}{60 \cdot 24 \cdot 360} \text{ (Jahre)}$$

30 wobei  $T_e$  die Entschlüsselungszeit (Jahre),  $T_s$  die  
Sperrzeit (Minuten) und  $N$  die Code-Permutationen sind.

Diese Parameter werden entsprechend dem sicherheits-  
technischen Bedürfnis so gewählt, daß die Entschlüsse-  
lungszeit beispielsweise ein mehr oder weniger großes  
Vielfaches der Gültigkeitsdauer des Identifikations-  
5 elements beträgt.

Die Sperrzeit  $T_s$  wird dabei im wesentlichen durch die  
Entladezeitkonstante des Zeitgliedes bestimmt. Da  
die beteiligten Entladewiderstände sehr hoch gewählt  
10 werden können, lassen sich auch bei Kondensatoren sehr  
kleiner Kapazität schon relativ lange Entladezeiten  
erzielen. Die wirksame Sperrzeit nach dem Auftreten eines  
Fehlersignals kann dadurch noch erheblich verlängert  
werden, wenn die bei Logikbausteinen übliche Schalt-  
15 schwellen mit Hilfe eines an den Impedanzwandler an-  
geschlossenen nicht gezeigten Komparators entsprechend  
niedrig gewählt wird.

Auf der anderen Seite ist aufgrund der geringen Kapa-  
20 zität des Kondensators und des niedrigen, im wesentli-  
chen durch den Durchgangswiderstand der Diode 8 beding-  
ten Aufladewiderstandes die Aufladezeit so gering, daß  
ein Betrüger praktisch keine Möglichkeit hat, den  
Prozeß, dessen Einleitung er zunächst einmal erkennen  
25 muß, zu unterbrechen. Die Erkennung dieses Prozesses  
ist auch deshalb schwierig, weil dazu der Aufladestrom  
von dem allgemeinen Betriebsstrom isoliert werden muß,  
was praktisch jedoch nicht möglich ist, weil auch der  
Betriebsstrom aufgrund der kontinuierlich ablaufenden

Vorgänge im integrierten Schaltkreis ständig mehr oder weniger starken Schwankungen ausgesetzt ist.

Die Fig. 3 zeigt eine Weiterbildung des in der Fig. 2  
5 gezeigten Zeitgliedes. Hier ist die Versorgungsleitung der Schaltung über einen weiteren Kondensator 12 und eine in Sperrrichtung geschaltete Diode 13 mit der Schaltungsmasse verbunden. Dieser Kondensator 12 kompensiert den in der Anfangsphase der Aufladung  
10 des Kondensators 7 auftretenden Stromimpuls, welcher theoretisch mit entsprechend hohem Aufwand in der in Fig. 2 gezeigten Schaltung detektierbar wäre. Auf der anderen Seite verhindert die Diode 13, daß eine negative Versorgung das Verhalten der Schaltung beein-  
15 flußt, wobei die an der Diode abfallende Restspannung mit Hilfe einer Diode 14 kompensiert wird.

Eine weitere Ausführungsform des erfindungsgemäßen Zeit-  
gliedes ist in der Fig. 4 gezeigt. Bei dieser Schal-  
20 tung wird im Fehlerfall ein interner Umladeprozess eingeleitet, der auf die extern zugängigen Anschlußleitungen des Identifikationselements keinen Einfluß hat. In diesem Fall ist parallel zu dem Kondensator 7 ein weiterer Kondensator 15 vorgesehen, der beim An-  
25 legen der Versorgungsspannung an das Identifikations-  
element über einen zu diesem Zeitpunkt geschlossenen Schalter 16 aufgeladen wird. Mit dem Auftreten eines Fehlerimpulses wird ein Flip-Flop 17 gesetzt, mit dessen Ausgangssignalen der Schalter 16 geöffnet und  
30 ein Schalter 18 geschlossen wird, so daß nunmehr der



- Kondensator 7 geladen wird, der die Sperrzeit einleitet. Während des Umladens sowie während der Dauer der Sperrzeit sind die Kondensatoren 7, 15 von der Versorgungsleitung entkoppelt, so daß weder der Aufladevorgang noch die Dauer der Sperrzeit beeinflussbar sind. Nach Ablauf der Sperrzeit wird das Flip-Flop 17 zurückgesetzt, so daß der alte Zustand wieder hergestellt ist.
- 10 Das erfindungsgemäße Zeitglied gemäß den Ausführungsformen von Fig. 2 - 4 kann auch dazu genutzt werden, um nach dem Auftreten eines Komparatorausgangssignals die Betriebsbereitschaft des Identifikationselements für einen vorgegebenen Zeitraum aufrecht zu erhalten.
- 15 Ein Problem bei der Handhabung der oben genannten Identifikationselemente besteht nämlich darin, daß die Code-Eingabe am Geldausgabeautomaten durchgeführt wird und deshalb grundsätzlich von fremden Personen ausgespäht werden kann. Dies gilt vor allem dann,
- 20 wenn die Automaten an stark frequentierten Orten aufgestellt sind.

- Es ist in diesem Zusammenhang schon vorgeschlagen worden, das Identifikationselement selbst mit einer mechanischen Code-Eingabemöglichkeit auszurüsten, die es dem Benutzer ermöglicht, unabhängig von Automaten seinen persönlichen Code einzustellen. Die Maßnahme erfüllt grundsätzlich ihren Zweck, bedingt jedoch einen relativ hohen technischen Aufwand und ist bei
- 30 Identifikationselementen in Form von Ausweiskarten

mit ihren vorgegebenen Abmessungen schlecht durchführbar. Außerdem erweist es sich als nachteilig, daß nach der Einstellung des Codes dieser am Identifikationselement ablesbar und damit für jedermann zugänglich ist.

Im Rahmen der vorliegenden Erfindung können diese Schwierigkeiten dadurch beseitigt werden, indem das oben erläuterte Zeitglied in der Weise genutzt wird, daß ein richtig eingegebener Code den Betrieb des Identifikationselements für einen vorgegebenen Zeitraum ermöglicht. Zur Code-Eingabe kann in diesem Fall ein persönliches Taschenterminal in der Bauart heute üblicher Taschenrechner verwendet werden. Dieses Gerät kann auch dazu genutzt werden, um andere Daten des Identifikationselements, beispielsweise den jeweiligen gültigen Kontostand in Erfahrung zu bringen. Nach der Eingabe des richtigen Codes an einem vom öffentlichen Geldausgabeautomaten entfernten Ort kann auf diese Weise erreicht werden, daß das Identifikationselement für einen vorgegebenen Zeitraum betriebsbereit ist, wobei die Betriebsbereitschaft durch eine geeignete Anzeige am Taschenterminal visuell erkennbar gemacht werden kann. Die durch mögliches Ausspähen am öffentlichen Geldausgabeautomaten gefährdete Code-Eingabe entfällt. Die Betriebsbereitschaft des Identifikationselements wird nach Beendigung der Transaktion am Geldausgabeautomaten automatisch gelöscht.

Eine vorteilhafte Kombination der zwei genannten

Funktionen des erfindungsgemäßen Zeitgliedes ist in Fig. 5 gezeigt. Dabei wird sowohl beim Auftreten eines Ja-Signals als auch beim Auftreten eines Nein-Signals des Komparators jeweils ein Zeitglied in der oben detailliert beschriebenen Weise aktiviert. Bei einem Nein-Signal wird das Zeitglied 1 angesteuert und die Funktion des Identifikationselements für einen vorgegebenen Zeitraum blockiert. Bei einem Ja-Signal wird hingegen ein Zeitglied 2 angesteuert, wodurch die Betriebsbereitschaft des Identifikationselements für einen vorbestimmten Zeitraum aufrecht erhalten wird.

Es laufen also unabhängig vom Ausgangssignal des Komparators innerhalb des Identifikationselements die gleichen Vorgänge ab. Der Betrüger hat somit keine Möglichkeit, die Sperrfunktion des Identifikationselements in irgendeiner Weise zu erfahren oder zu manipulieren, weil er aus den nach einer Code-Eingabe extern möglicherweise auftretenden Änderungen der Betriebsdaten keine Rückschlüsse auf die tatsächliche Komparator-Entscheidung ziehen kann. Auf der anderen Seite kann der rechtmäßige Benutzer nach vorheriger Code-Eingabe ohne weitere Code-Eingabe an dem Automaten durch einfaches Einschieben der Karte die gewünschte Funktion auslösen.

Bei den bisher gezeigten Ausführungsformen der Erfindung wird das Identifikationselement nach jeder Fehleingabe für einen vorbestimmten Zeitraum blockiert.

Um Korrekturen am Geldausgabeautomaten oder am persönlichen Taschenterminal trotzdem zu ermöglichen, kann am jeweiligen Gerät eine Taste vorgesehen sein, mit deren Hilfe ein versehentlich falsch eingegebener Code vor der entgeltigen Verarbeitung im  
5 Gerät annulliert wird.

Eine andere Möglichkeit, versehentlich begangene Fehleingaben zuzulassen, zeigt das Ausführungsbeispiel von Fig. 6. In diesem Fall erfolgt die Blockierung des Identifikationselements erst nach der  
10 zweiten oder dritten Fehleingabe, welche durch einen Zähler 20 ermittelt wird. Dabei ist ferner ein Schwellwertschalter 21 vorgesehen, der ebenfalls  
15 das Identifikationselement sperrt, wenn die Versorgungsspannung einen vorgegebenen, die Funktion des Zählers 20 sicherstellenden Wert unterschreitet. Auf diese Weise kann verhindert werden, daß ein Betrüger durch Abschalten der Versorgungsspannung die Zählerinformation löscht, bevor dieser die zulässige Fehlerzahl  
20 erreicht hat und damit die Sperrfunktion auslösen kann. Schließlich ist noch eine Steuerlogik 22 vorgesehen, welche ein Freigabesignal erzeugt, das bei Vorhandensein des Ausgangssignals des Schwellenwertschalters  
25 21 eine Aktivierung des Zeitgliedes erlaubt. Dieses Freigabesignal erscheint unmittelbar, nachdem das Identifikationselement zu Beginn der Transaktion an die Versorgungsspannung gelegt wird, und verschwindet, sobald der richtige Code eingegeben wurde. Auf diese  
30 Weise kann erreicht werden, daß das Identifikationselement nach dem Abschalten der Versorgungsspannung

- 20 -

im Anschluß an eine ordnungsgemäße Transaktion nicht  
blockiert wird.

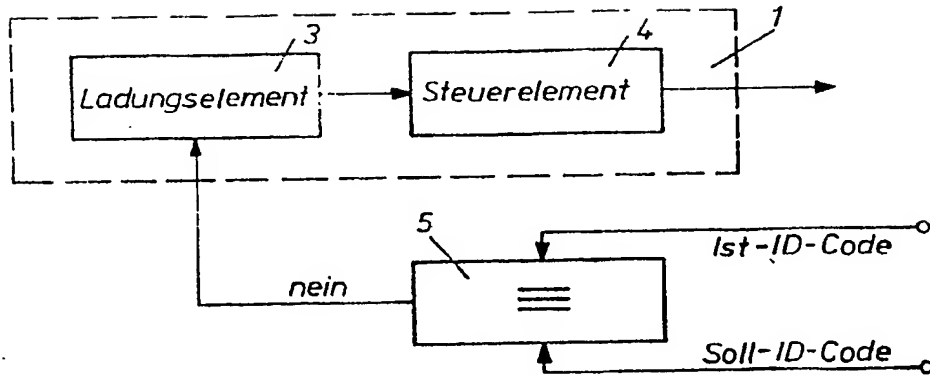


Fig. 1

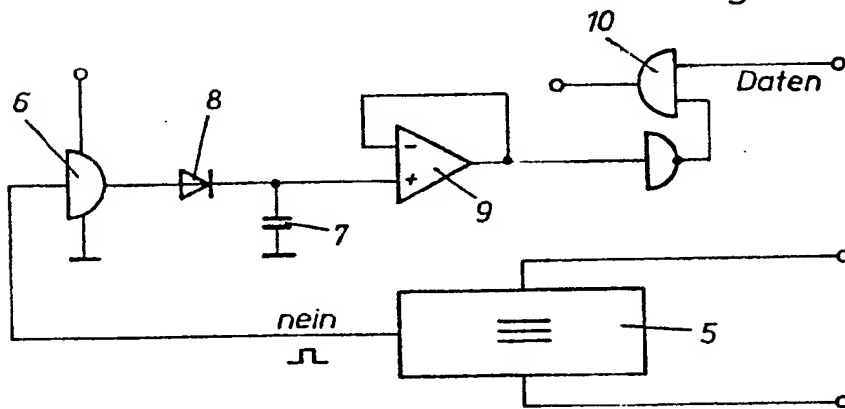


Fig. 2

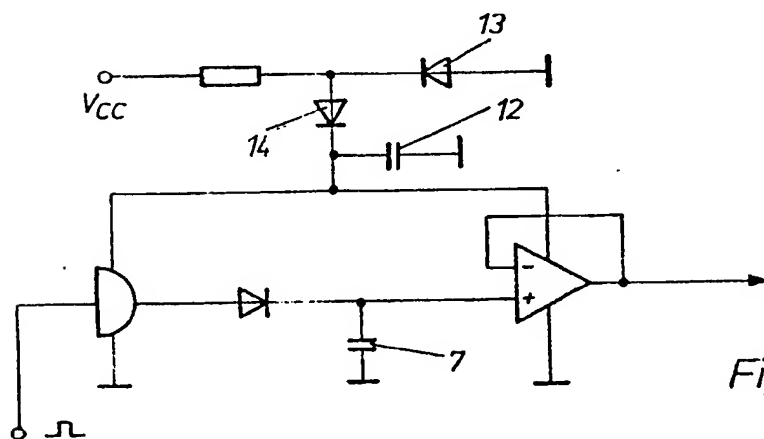
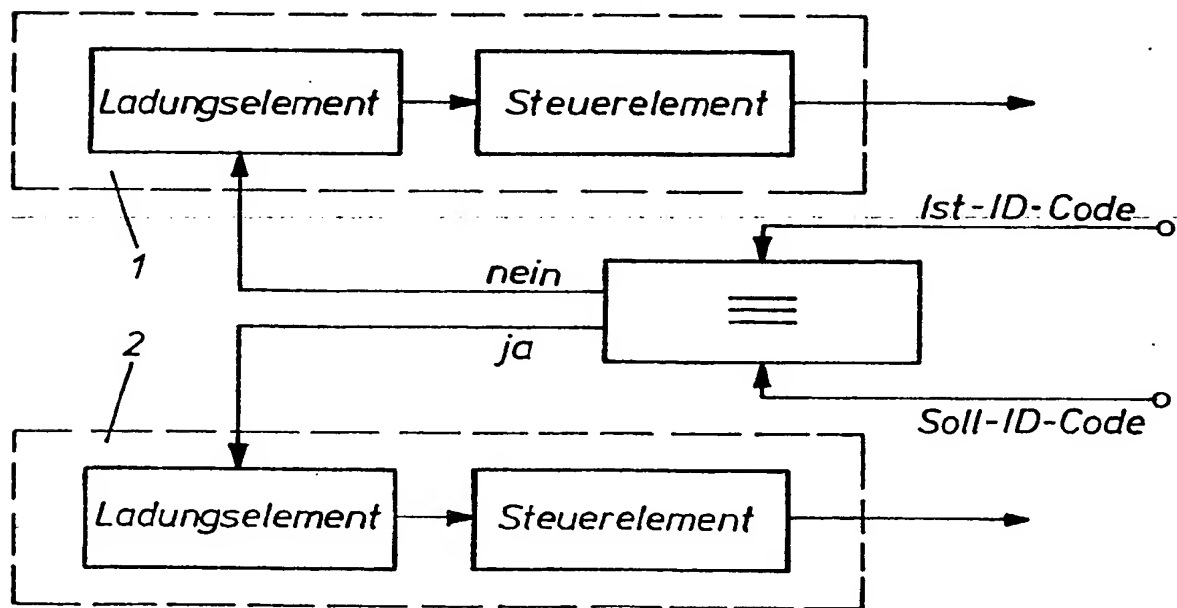
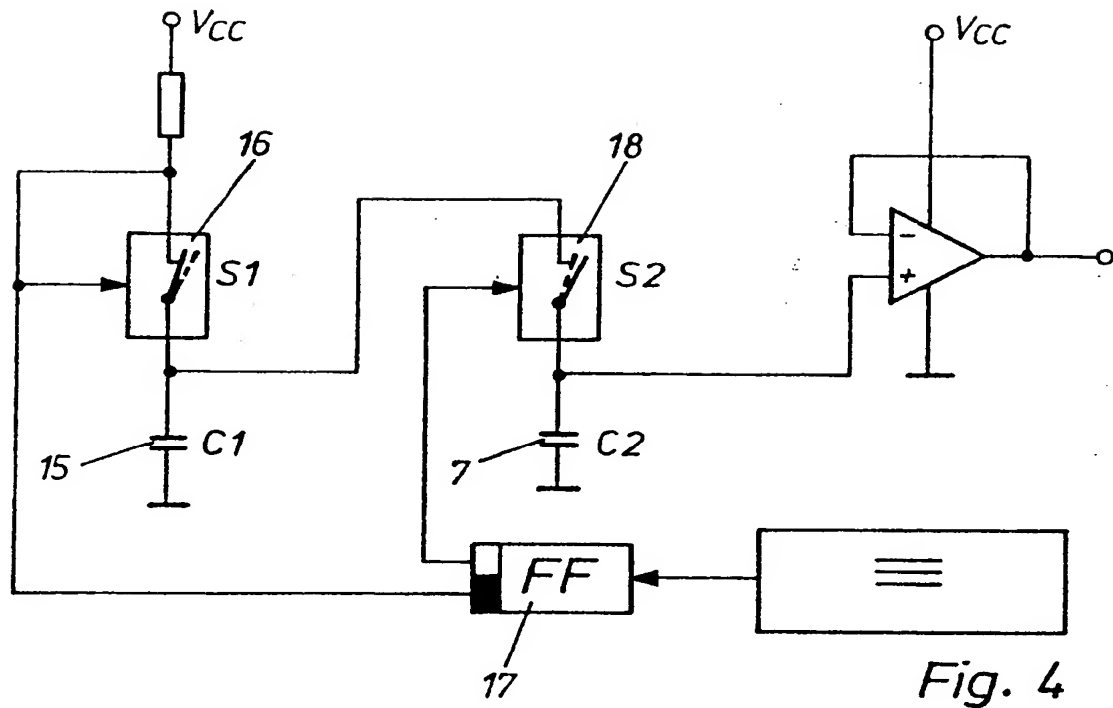


Fig. 3

- 21 -



- 22 -

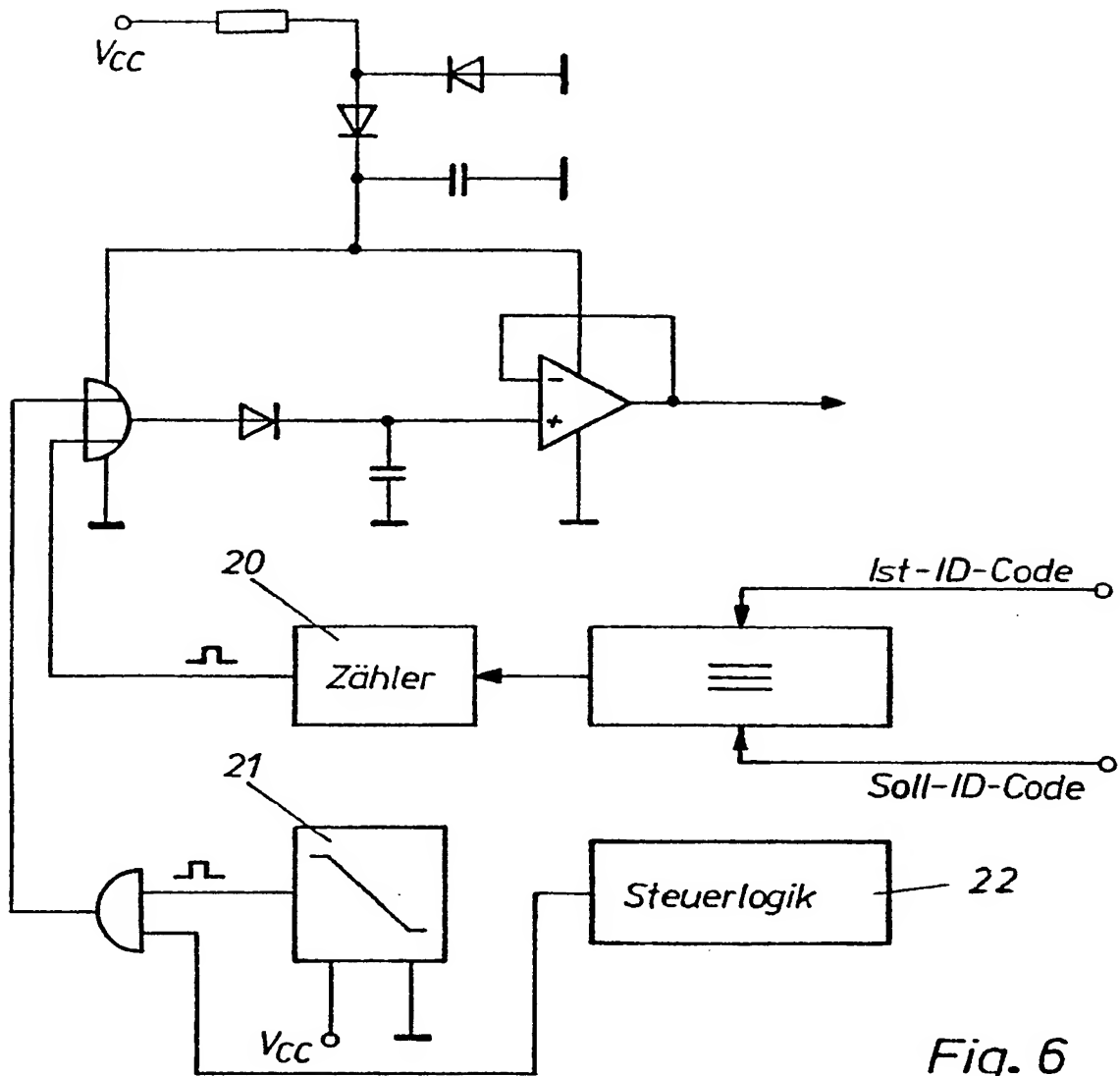


Fig. 6